Post Date: 2026/05/13

□Vulnerability Alert□Critical Security Vulnerability in Palo Alto Networks PAN-OS (CVE-2026-0300)

- Subject: □Vulnerability Alert□Critical Security Vulnerability in Palo Alto Networks PAN-OS (CVE-2026-0300)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert: TWCERTCC-200-202605-00000002
  - A buffer overflow vulnerability (CVE-2026-0300, CVSS: 9.3) exists in the User-ID authentication portal service of PAN-OS, the firewall operating system of Palo Alto Networks. This vulnerability allows an unauthenticated attacker to execute arbitrary code with root privileges on PA-series and VM-series system firewalls by sending specially crafted data.
- Affected Platforms:
  - Versions prior to PAN-OS 12.1.4-h5 (exclusive)
  - Versions prior to PAN-OS 12.1.7 (exclusive)
  - Versions prior to PAN-OS 11.2.4-h17 (exclusive)
  - Versions prior to PAN-OS 11.2.7-h13 (exclusive)
  - Versions prior to PAN-OS 11.2.10-h6 (exclusive)
  - Versions prior to PAN-OS 11.2.12 (exclusive)
  - Versions prior to PAN-OS 11.1.4-h33 (exclusive)
  - Versions prior to PAN-OS 11.1.6-h32 (exclusive)
  - Versions prior to PAN-OS 11.1.7-h6 (exclusive)
  - Versions prior to PAN-OS 11.1.10-h25 (exclusive)
  - Versions prior to PAN-OS 11.1.13-h5 (exclusive)
  - Versions prior to PAN-OS 11.1.15 (exclusive)
  - Versions prior to PAN-OS 10.2.7-h34 (exclusive)
  - Versions prior to PAN-OS 10.2.10-h36 (exclusive)
  - Versions prior to PAN-OS 10.2.13-h21 (exclusive)
  - Versions prior to PAN-OS 10.2.16-h7 (exclusive)
  - Versions prior to PAN-OS 10.2.18-h6 (exclusive)
- Recommended Actions:
  - Apply patches according to the solutions released on the official website: https://security.paloaltonetworks.com/CVE-2026-0300
- Reference Materials:
  1. https://www.twcert.org.tw/tw/cp-169-10898-012f2-1.html

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260513_34

Last update: **2026/05/13 16:26**